OIPE JC101
FEB 28 2005
PATENT & TRADEMARK OFFICE

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:)
)
Thomas D. Ashoff et al.) Examiner: Ali M. Mashaal
)
Serial No.: 09/495,157) Group Art Unit: 2136
)
Filed: January 31, 2000) Docket: 105.201US1
)
For: SYSTEM, METHOD AND COMPUTER PROGRAM PRODUCT FOR AUTHENTICATING USERS USING A LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL (LDAP) DIRECTORY SERVER

APPELLANTS' BRIEF ON APPEAL UNDER 37 C.F.R. 41.37(c)

Mail Stop Appeal Brief- Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This Brief is presented in support of the Notice of Appeal mailed July 16, 2004, from the final rejection of claims 1-17 of the above-identified application, as set forth in the Final Office Action mailed February 18, 2004. A copy of the claims being appealed is enclosed as Appendix I.

The Commissioner of Patents and Trademarks is hereby authorized to charge Deposit Account No. 19-0743 in the amount of 250.00 which represents the requisite fee set forth in 37 C.F.R. § 41.2(b)(2).

Appellants respectfully request consideration and reversal of the Examiner's rejections of pending claims 1-17.

03/01/2005 AWONDAF1 00000053 190743 09495157
01 FC:2402 250.00 DA

APPELANTS' BRIEF ON APPEAL UNDER 37 C.F.R. 41.37(c)

TABLE OF CONTENTS

1. REAL PARTY IN INTEREST

The Real Party in Interest of the above-captioned patent application is Secure Computing Corporation, the assignee of the application.

2. RELATED APPEALS AND INTERFERENCES

There are no related appeals or interferences for the above-referenced patent application.

3. STATUS OF CLAIMS

The present application was filed on January 31, 2000 with claims 1-17. A non-final Office Action was mailed September 10, 2003. A Final Office Action was mailed February 18, 2004. Claims 1-17 (Appendix I, Claims) stand rejected under 35 U.S.C. §103(a), remain pending, and are the subject of the present appeal.

4. STATUS OF AMENDMENTS

Appellants have not filed an amendment subsequent to the mailing of the Final Office Action on February 18, 2004.

5. SUMMARY OF CLAIMED SUBJECT MATTER

According to one embodiment, the present invention relates to a system (such as reference numeral 300, Figure 3) for authorizing client (such as reference numeral 102a, Figure 3) access to a network resource (such as reference numeral 118, Figure 3). The system includes a server (such as reference numeral 106, Figure 3; page 7, lines 11-17) that has at least one directory (such as reference numeral 204, Figure 3; page 7, lines 11-17) that can be accessed using a network protocol. The directory is configured to store information concerning an entity's organization (see Figure 4 generally, and page 7, lines 11-17). The system also includes a firewall (such as reference numeral 110, Figure 3; page 9, lines 1-3) that is configured to intercept network resource requests from a plurality of client users. The firewall is operative to authorize a network resource request based upon a comparison (page 9, lines 10-19) of the contents of at least part of one or more entries in the at least one directory to an authorization filter (see page 11, lines 7-15 for discussion relating to authorization filters). The authorization filter is generated based on a directory schema that is predefined by the entity (page 12, line 14-21).

According to another embodiment, the present invention relates to an authentication method (the method is represented by reference numerals 302, 304, 306, 308, and 310 in Figure 3) executed by a firewall (such as reference numeral 110 in Figure 3). The method includes receiving a network authorization request (such as reference numeral 304, Figure 3; page 8, line 20-page 9, line 2) from a client user (such as reference numeral 102a in Figure 3; page 8, line 20-page 9, line 2). The method also includes querying (reference numeral 306, Figure 3; page 9, lines 10-19), using a network protocol, at least one directory (reference numeral 204, Figure 3; page 9, lines 10-19) that is configured to store information concerning an entity's organization (see Figure 4, generally; page 7, lines 11-17). The query is based upon an authorization filter (see page 11, lines 7-15 for discussion relating to authorization filters) that is generated based on a directory schema that is predefined by said entity (page 12, line 14-21). The method further includes determining, based on the results of the query (reference numeral 308, Figure 3; page 9, lines 10-19), whether the contents of at least part of one or more entries in said at least one directory satisfy the authorization filter (page 9, lines 10-19). Finally, the method includes permitting the network resource request through the firewall if the authorization filter is satisfied (page 9, lines 17-19).

According to another embodiment, the present invention relates to a program product for enabling a processor in a computer system to implement an authentication process (the process is represented by reference numerals 302, 304, 306, 308, and 310 in Figure 3). The program product includes a computer usable medium having computer readable program code embodied in the medium for causing a program to execute on the computer system. The program code includes a first computer readable program code for enabling the computer system (such as reference numeral 110, Figure 3; page 8, line 20-page 9, line 2) to receive a network request from a client user (such as reference numeral 102a, Figure 3; page 8, line 20-page 9, line 2). The program code also includes a second computer readable program code for enabling the computer system to query (reference numeral 306, Figure 3; page 9, lines 10-19), using a network protocol, at least one directory (reference numeral 204, Figure 3; page 9, lines 10-19) that is configured to store information concerning an entity's organization (see Figure 4, generally; page 7, lines 11-17). The query is based upon an authorization filter (see page 11, lines 7-15 for discussion relating to authorization filters) that is generated based on a directory schema that is predefined by said entity (page 12, line 14-21). The program code also includes a third computer readable program code for enabling the computer system to determine, based on the results of the query (reference numeral 308, Figure 3; page 9, lines 10-19), whether the contents of at least part of one or more entries in the at least one directory satisfy the authorization filter (page 9, lines 10-19). Finally, the program code also includes fourth computer readable program code for enabling the computer system to permit the network resource request through the firewall if the authorization filter is satisfied (page 9, lines 17-19).

This summary does not provide an exhaustive or exclusive view of the present subject matter, and Appellant refers to the appended claims and their legal equivalents for a complete statement of the invention.

6. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Whether independent claims 1-17 have been erroneously rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,131,120 to *Reid* in view of the *Microsoft Computer Dictionary* 1997, in further view of *Check Point Account Management Client*, Version 1.0, September 1998, and in view of other art relevant to the dependent claims (not at issue herein).

7. ARGUMENT

A. The Law Applicable Under 35 U.S.C. §103

MPEP §2142 states the basic applicable law governing obviousness of claimed subject matter:

> To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991).

B. Introduction

Claims 1-17 each include a limitation requiring a comparison between data from a directory and an authorization filter. None of the prior art cited in the Office actions to date teach or suggest such a comparison. For this reason, claims 1-17 should have been allowed.

C. Appellants' Invention

Appellants describe, and claim in claims 1-17, a firewall that communicates with a directory hosted on a server to determine if a network resource access request should be authorized or denied. Figure 1 depicts an example of such a firewall. The example presented in Figure 1, and discussed throughout, is intended to generally familiarize the reader with Appellants' invention, and is not intended to be an exhaustive description.

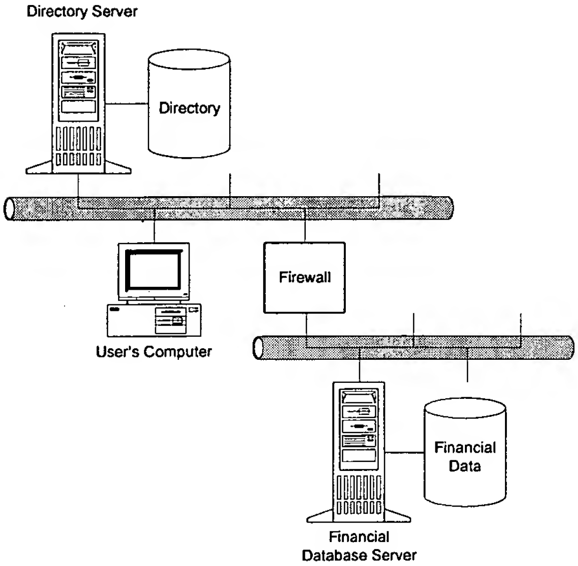

Figure 1

As can be seen from Figure 1, a firewall is interposed between user's computer and a financial database server, an example of a "network resource." Thus, any attempts to access the financial database server must pass through the firewall. The firewall intercepts the computer's first attempt to access the financial database server. See Application, page 9, lines 1-3.

In the wake of having intercepted the request, the firewall performs an operation to identify the user logged on to the computer from which the request emanated. See Application, page 9, lines 3-13. Based upon the identity of the user, the firewall queries a directory stored on a server to learn of attributes describing the user. Id.

A directory is similar to a database, in that it stores data that may be retrieved via query, but a directory is tailored to be read from more than it is written to. In the case of this invention, the directory stored on the server contains information concerning the organization of the entity employing the computer user. See Application, page 7, lines 11-17. For example, the directory may be organized as shown in Figure 2.

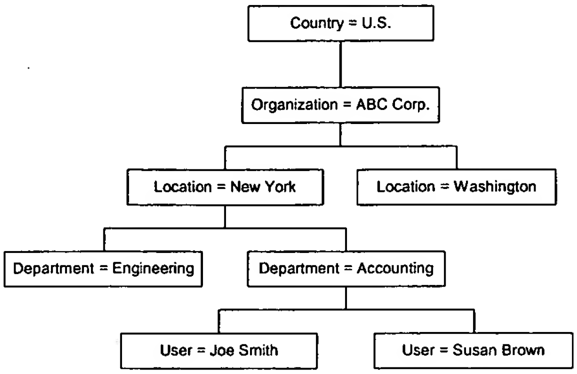

Figure 2

Thus, by virtue of querying such a directory with a given user's name, the firewall may obtain the department employing the user, the location in which the user is employed, the name of the organization employing the user, and the country in which the user is employed. Each of these pieces of information is an attribute describing the user.

After having obtained the user's attributes, the attributes are compared to an authorization filter. At its simplest, an authorization filter is an attribute and value pair. In the case of this example, the filter may be "Department = Accounting" (i.e., the user must work for the accounting department to be able access the financial database server). The firewall authorizes or denies the request on the basis of this comparison.

The act of comparing the authorization filter to data obtained from the directory is an element of every independent claim. For example, claim 1 requires "a comparison of the contents of at least part of one or more entries in said at least one directory to an authorization filter." Similarly, claims 8 and 17 require determining "whether the contents of at least part of one or more entries in said at least one directory satisfy said authorization filter." Thus, the independent claims require the general structure depicted in Figure 3, below

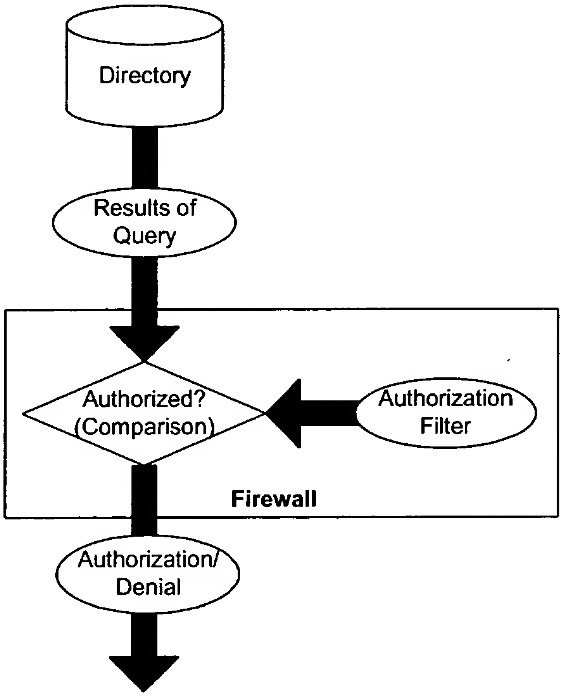

Figure 3

As shown in Figure 3, the claims require the authorization process to include a comparison of data returned from a query of the directory to an authorization filter.

D. The Prior Art

1. Summary of the Cited Prior Art

The prior art cited against the independent claims includes: (1) U.S. Patent No. 6,131,120 to *Reid*; (2) *Microsoft Computer Dictionary* 1997; and (3) *Check Point Account Management Client*, Version 1.0, September 1998. Of these, only the teachings of *Reid* are at issue. Briefly, *Microsoft Computer Dictionary* is cited to for its definition of the term "firewall," in order to support the proposition that the routers in *Reid* may be thought of as firewalls, because of the functionality they provide (Appellants do not dispute this). *Check Point Account Management Client* is a software manual, and is cited to support the proposition that it would have been obvious to modify the directory described in *Reid* to store information concerning an entity's organization (for the purposes of this appeal only, Appellants do not dispute this).

2. U.S. Patent No. 6,131,120 to *Reid*

Reid teaches a system whereby each router or gateway (collectively referred to herein as a router) stores a router access list. A router access list is a list of names and addresses of users and the destinations they are permitted to access. See Final Office Action, page 2 ("Each RAL [router access list] . . . includes the names and addresses of users and the destinations they are allowed to reach."). According to the scheme taught in *Reid*, a router intercepts a network resource access request, and extracts the requesting computer's address and requested destination address. If the router access list indicates that the requesting computer is permitted to access the requested address, the access is authorized, otherwise it is denied. See Final Office Action, pages 2-3.

The router access list taught by *Reid* is created automatically by a software application running on a server that stores a directory. See *Reid*, col. 8, lines 23-28. The directory contains, amongst other entries, the name and access privileges assigned to each user. See *Reid*, col. 8, lines 6-11 and 23-27. For each router in an organization's system, the application creates an appropriate router access list and sends the list to the router. See *Reid*, col. 8, lines 21-34.

The general structure of the authorization process described by *Reid* is depicted in Figure 4, below.

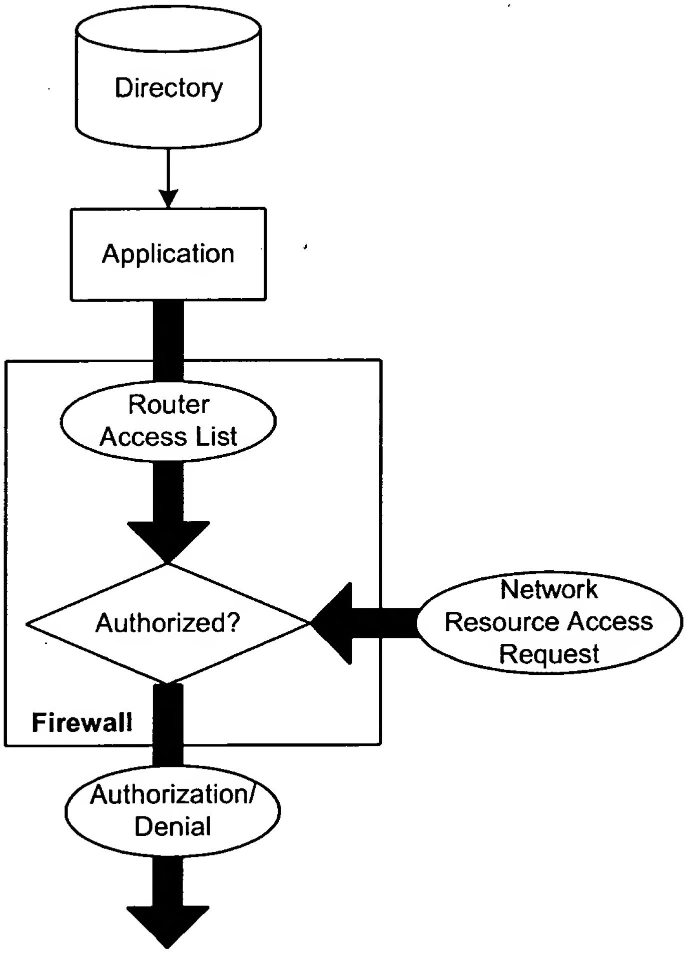

Figure 4

E. Brief Summary of Prosecution

The above-captioned application was filed on January 31, 2000. A first Office action was mailed on September 10, 2003 (claims 1-17 were rejected under 35 U.S.C. §103(a) as being obvious). Appellants filed a response on January 16, 2004. A final Office action was mailed on February 18, 2004 (claims 1-17 remained rejected under 35 U.S.C. §103(a), although the premise of the rejection changed). Finally, Appellants filed a notice of the present appeal on July 16, 2004.

F. Appellants' Rebuttal of the Rejections of the Independent Claims

1. The Initial Office Action

In a first Office action mailed September 10, 2003, the independent claims were rejected as being obvious in light of *Reid* and other prior art, the teachings of which are not presently at issue.

As stated above, each of the independent claims requires the act of comparing an authorization filter to data obtained from the directory. On its face, *Reid* wholly lacks any teaching or suggestion of such an act. To formulate his initial rejection, the Examiner seized upon an incorrect interpretation of *Reid.* Specifically, the Examiner assumed the existence of two separate unarticulated steps in Reid: (1) that the firewall transmitted access criteria, which the Examiner likened to an authorization filter, to the directory; and (2) that a comparison between the access criteria and the contents of the directory was performed as a part of the process of producing the router access lists. According to the Examiner,

> . . . in order for the directory to generate the appropriate [router] access list, each router/gateway must have transmitted its access criteria to the directory. The examiner further asserts that this criteria is an authorization filter and that in order for the directory to send back a correct access list, some comparison must have been made with directory entries and the router/gateway criteria (authorization filter).
>
> Initial Office Action, page 5.

Thus, according to the Examiner, the authorization process of *Reid* includes the extra—albeit completely unmentioned—steps, shown in dashed lines, depicted in Figure 5, below.

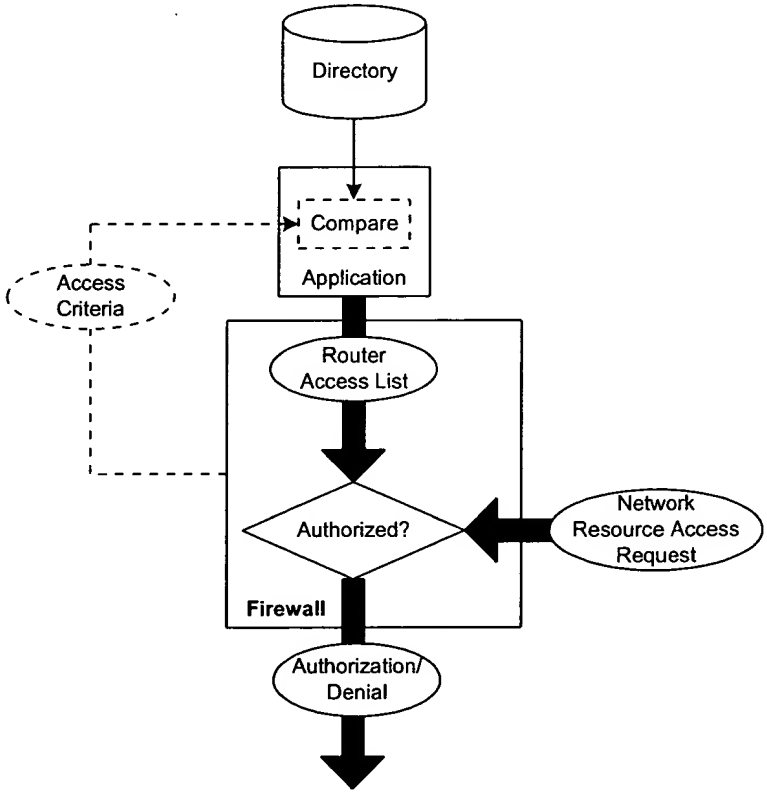

Figure 5

In a response filed January 16, 2004, Appellants argued that neither the "access criteria," nor the comparison step are referred to, or even hinted at, by the text of *Reid*. Further, Appellants went on to argue that the text of *Reid* plainly contradicts the very notion of their existence. Appellants argued that the router access lists of *Reid* are generated on the sole basis of the contents of the directory. Put simply, the application reads the directory and creates the router access lists. The process involves no transmission of access criteria, nor does it involve a comparison between access criteria and the contents of the directory.

In support of their position, Appellants cited column 6, lines 23-25 of *Reid* (emphasis added), which states that entries in the directory control the entire network:

> Because the directory knows the location and IP address of each user, and the location and IP address of each router/gateway, a directory application can periodically populate the RAL [router access list] in each router/gateway on the network using LDAP. Entries in the directory thereby control the entire network and the network router/gateway configuration management is automated.

The Examiner seems to have accepted this argument, because, in authoring his final rejection, he has altered his interpretation of *Reid*, in order to find a new way in which one might understand it to include a comparison between an authorization filter and data obtained from the directory.

2. The Final Office Action

In authoring his final rejection, the Examiner has reinterpreted *Reid* to find the missing element in a routine act performed by virtually every router that has been configured to act as a firewall: the act of comparing a network access request to a router access list. According to the Examiner, the routers of *Reid*

> compare[] the requesting device's address and requested destination to that information in the router/gateway which was provided by the directory server [i.e., the router access list], in order to determine whether the requesting device should be allowed/denied access. Therefore, the router/gateway clearly contains an authorization filter by which it can make a comparison of the content of at least

> part of one or more entries in the directory to determine which traffic may be allowed to pass through to a given destination.

Final Office Action, pages 2-3.

The Examiner's latest interpretation of *Reid* still falls short of requirements posed by each of Appellants' claims. The independent claims require a comparison between an authorization filter and at least a portion of an entry in the directory. For example claims 1-7 require "a comparison of the contents of at least part of one or more entries in said at least one directory to an authorization filter." (Claims 8 through 17 include similar language.) The Examiner's interpretation does not even purport to find such a comparison in *Reid*. Instead, the Examiner's interpretation of *Reid* yields a comparison between a router access list (which the Examiner likens to an authorization filter) and address data extracted from the network access request. The difference between the claimed invention and the Examiner's latest interpretation of Reid is depicted in Figure 6.

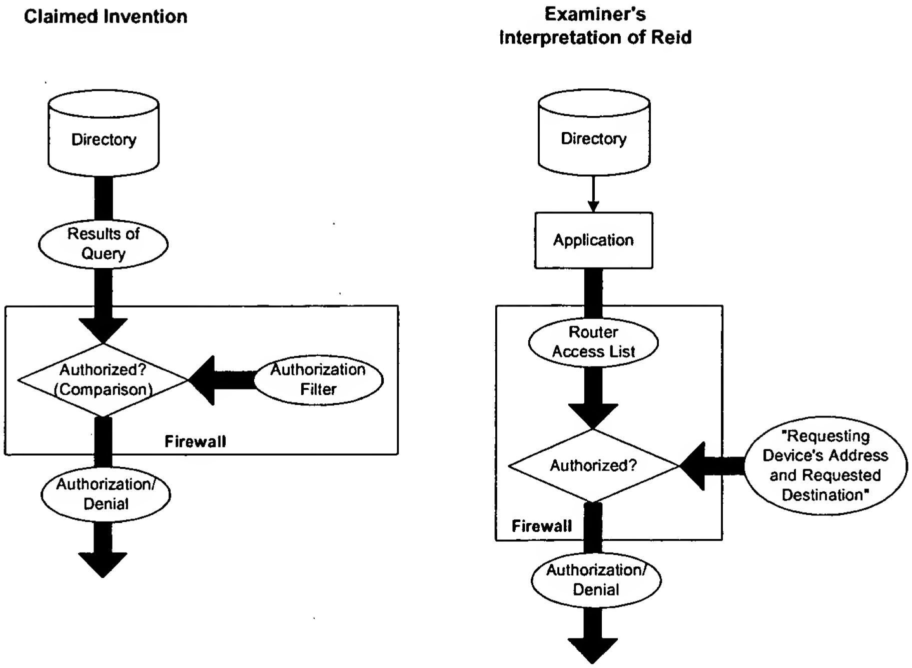

Figure 6

As can be seen from Figure 6, the claimed invention includes a comparison between an authorization filter and at least a portion of an entry from the directory (i.e. the "results of query" shown in Figure 6). Turning to *Reid*, on the other hand, even if one accepts the Examiner's position that a router access list is an authorization filter, the comparison does not occur between the proper subjects. Therein, at stated in the Examiner's Response to Arguments, the comparison occurs between the router access list (asserted to be an authorization filter) and "the requesting device's address and requested destination." See Final Office Action, page 2. The requesting device's address and requested destination are units of information extracted from the network resource access request—not from the directory. Therefore, at best, the comparison in *Reid* occurs between an authorization filter (router access list) and information extracted from the network resource access request[1], not the query results as described by Appellants and stated in claims 1-17. Plainly, such a comparison does not rise to textual requirements presented in claims 1-17.

[1] For the present purposes, Appellants take no position regarding whether a router access list may be properly characterized as an authorization filter. To the extent Appellants have appeared to acquiesce in this portrayal, Appellants have done so in order to present the Examiner's interpretation of *Reid*—not to endorse the Examiner's interpretation.

G. Conclusion

The prior art cited against claims 1-17 fails to teach or suggest a comparison between an authorization filter and data obtained from a directory. This act is required by each of the rejected claims. The record fails to present any motivation for one to modify *Reid* to include such a step. Indeed, it is not clear how *Reid* could so be modified, without altering the theory of operation of the firewall function presented therein. For at least this reason, the rejection of claims 1-17 is improper, and the rejection should be withdrawn.

Respectfully submitted,

THOMAS D. ASHOFF ET AL.

By their Representatives,

SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH, P.A.
P.O. Box 2938
Minneapolis, MN 55402

Date 22 Feb. 2004 By

Nicholas P. Johns
Reg. No. 48,995

CERTIFICATE UNDER 37 CFR 1.8: The undersigned hereby certifies that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail, in an envelope addressed to: Mail Stop Appeal Brief, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on this 22 day of February, 2005.

Peter Rebuffoni
Name

Signature

APPENDIX I

THE CLAIMS ON APPEAL

1. (Previously Presented) A system for authorizing client access to a network resource, comprising:

a server having at least one directory that can be accessed using a network protocol, said at least one directory being configured to store information concerning an entity's organization; and

a firewall that is configured to intercept network resource requests from a plurality of client users, said firewall being operative to authorize a network resource request based upon a comparison of the contents of at least part of one or more entries in said at least one directory to an authorization filter, wherein said authorization filter is generated based on a directory schema that is predefined by said entity.

2. (Original) The system of claim 1, wherein said at least one directory is a lightweight directory access protocol directory.

3. (Original) The system of claim 1, wherein said authorization filter is specified using a graphical user interface.

4. (Original) The system of claim 1, wherein said authorization filter implements a per-user authentication scheme.

5. (Original) The system of claim 1, wherein said authorization filter implements a per-service authentication scheme.

6. (Original) The system of claim 1, wherein said firewall and said directory communicate using secure socket layer communication.

7. (Original) The system of claim 1, wherein said firewall is configured to query multiple directories.

8. (Original) An authentication method at a firewall, comprising the steps of:

(a) receiving a network resource request from a client user;

(b) querying, using a network protocol, at least one directory that is configured to store information concerning an entity's organization, wherein said query is based upon an authorization filter that is generated based on a directory schema that is predefined by said entity;

(c) determining, based on the results of said query, whether the contents of at least part of one or more entries in said at least one directory satisfy said authorization filter; and

(d) permitting said network resource request through said firewall if said authorization filter is satisfied.

9. (Original) The method of claim 8, wherein step (b) comprises the step of querying said at least one directory using a lightweight directory access protocol.

10. (Original) The method of claim 8, further comprising the step of specifying an authorization filter using a graphical user interface.

11. (Original) The method of claim 10, wherein said specifying step comprises the step of specifying an authorization filter that implements a per-user authentication scheme.

12. (Original) The method of claim 10, wherein said specifying step comprises the step of specifying an authorization filter that implements a per-service authentication scheme.

13. (Original) The method of claim 8, wherein step (b) comprises the step of querying said directory using secure socket layer communication.

14. (Original) The method of claim 8, wherein step (b) comprises the step of querying multiple directories.

15. (Original) The method of claim 8, wherein step (a) comprises the step of receiving a network resource request from a client user at an internal network.

16. (Original) The method of claim 8, wherein step (a) comprises the step of receiving a network resource request from a client user at an external network.

17. (Original) A computer program product for enabling a processor in a computer system to implement an authentication process, said computer program product comprising:

a computer usable medium having computer readable program code embodied in said medium for causing a program to execute on the computer system, said computer readable program code comprising:

first computer readable program code for enabling the computer system to receive a network resource request from a client user;

second computer readable program code for enabling the computer system to query, using a network protocol, at least one directory that is configured to store information concerning an entity's organization, wherein said query is based upon an authorization filter that is generated based on a directory schema that is predefined by said entity;

third computer readable program code for enabling the computer system to determine, based on the results of said query, whether the contents of at least part of one or more entries in said at least one directory satisfy said authorization filter; and

fourth computer readable program code for enabling the computer system to permit said network resource request through said firewall if said authorization filter is satisfied.